UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/524,057	12/29/2005	Tai Pang Chen	212/688US	4440

23371 7590 12/22/2010

CROCKETT & CROCKETT, P.C.
26020 ACERO
SUITE 200
MISSION VIEJO, CA 92691

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/22/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/524,057	CHEN ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 November 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1, 2, 3, 5, 7 -25, 27, 29 - 43 and 45 -61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 3, 5, 7 -25, 27, 29 - 43 and 45 -61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/22/2010 has been entered. Claims 1, 24, 38 and 49 are amended. Claims 1, 2, 3, 5, 7 -25, 27, 29 - 43 and 45 -61 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

1. Claims 1-3, 5, 7-25, 27, and 29-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamid (US Patent No. 2003/0223624) in view of Larsson et al (US Patent Publication No. 2004/0215615 and Larsson hereinafter).

2. As to claim 1, Hamid teaches a method of authenticating a user according to a biometrics parameter of the user presented at an authentication device on a user-presented device on which is stored a biometrics identification template (i.e., fingerprint template) divided into a secure portion (e.g., private portion) and an open portion (e.g., public portion) [par. 27], the method comprising: transmitting to a client terminal (i.e., smart card reader interface) data derived from said user biometrics parameter at the authentication device [par. 27], wherein the open 3ortion (e.g., public portion) is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template [par. 27]; transmitting from a user-presented device (i.e., smart card) to the client terminal only the open portion (e.g., public portion) of the said biometrics identification template held on the user-presented device (e.g., smart card) (i.e., ... Hamid teaches transmitting from a smart card a public portion to a host computer [par. 27], at the client terminal (e.g., host processor) implementing a first stage of an biometric identity authentication process between said

derived data and said open portion to produce intermediate results and transmitting the intermediate results of said biometric authentication process to the user-presented device (i.e., ... teaches a host processor align sensed image with portion of fingerprint received. Extracting the aligned image and creating a image portion [26, 27, fig. 3]), wherein said intermediate results (e.g., image portion) comprise parameters for alignment of said derived data and said biometric identification template (i.e., ... teaches providing a image portion extracted from an aligned image from which a derived private portion was constructed [par. 27]); and at the user-presented device (i.e., smart card) implementing a second stage of the biometric identity authentication process to complete the biometric identity authentication process using said intermediate results and said secure portion and issuing a biometric authentication result based thereon (e.g., ... teaches a smart card comparing a image portion with a private portion [29, fig. 3]). Hamid discloses the use of a public portion (e.g., open portion) in paragraphs 26 & 27, however Hamid does not expressly teach that the open portion is the portion containing data insufficient to construct a fake template that would allow an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template. The Examiner contends applicant discloses in paragraph 79 of applicant's original disclosure that the open portion is compressed data stored on the smart card. This compressed data contains less crucial information. The Examiner respectfully submits at the time of applicant's original filings Larsson disclosed a template residing on a smart card with both processed and compressed data [par. 37]. Therefore given Hamid's use of a smart card

containing biometric data a person having ordinary skill in the art would have recognize the advantage of modifying Hamid to enhance the security of the stored biometric data on the smart card with the feature of compressed data as disclosed by Larsson.

3. As to claim 2, Hamid teaches a method of registration of a user according to a biometrics parameter of the user presented at an authentication device [par. 26], the method comprising; transmitting to an authorized client terminal) data said user biometrics parameter obtained at the authentication device [par. 26]; at the authorized client terminal, dividing the biometrics identification template computed into secure portion and open portion [par. 26]; transmitting from the authorized client terminal (e.g., imaging device), to a user- presented device both the open portion and the secure portion of a biometrics identification template [par. 26], storing the said template consisting of open and secure portions on the user- presented device [par. 26]. Hamid discloses the use of a public portion (e.g., open portion) in paragraphs 26 & 27 however Hamid does not expressly teach that the open portion is the portion containing data insufficient to construct a fake template that would allow an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template. The Examiner contends applicant discloses in paragraph 79 of applicant's original disclosure that the open portion is compressed data stored on the smart card. This compressed data contains less crucial information. The Examiner respectfully submits at the time of applicant's original filings Larsson disclosed a template residing on a smart card with both processed and compressed data [par. 37].

Therefore given Hamid use of a smart card containing biometric data a person having ordinary skill in the art would have recognize the advantage of modifying Hamid to enhance the security of the stored biometric data on the smart card with the feature of compressed data as disclosed by Larsson.

4. As to claim 3, Hamid teaches a method where the secure portion of the biometrics identification template is the portion containing data unauthorized modification of which may cause an impostor to be incorrectly authenticated as a genuine user (i.e., Hamid teaches user biometric characteristics stored on a portable standalone device [fig. 1]).

5. As to claim 4, Cancelled.

6. As to claim 5, Hamid teaches a method where the biometrics parameter is a Fingerprint (103, 104, fig. 4).

7. As to claim 6, Cancelled. 9. As to claim 7, Hamid teaches a method where the first stage of said biometric identity authentication process implemented at the client terminal comprises locating unique features using the data derived from the user biometrics parameter and aligning them with said predetermined number of unique features from the identification template held on the user-presented device (106, fig. 4).

8. As to claim 8, Hamid teaches a method where the second stage of the said identity authentication process implemented on the user-presented device (i.e., smart card) is implemented using a local executable matching program (i.e., application) stored on the device (109, 110, fig, 4).

9. As to claim 9, Hamid teaches a method where the first stage of the identity authentication process implemented at the client terminal is implemented using a client executable matching program (106, 107, fig. 4).

10. As to claim 10, Hamid teaches a method where the client executable matching program is stored on the user-presented device (i.e., smart card) or the authentication device and is transmitted to the client terminal at the time of authentication [par. 23].

11. As to claim 11, Hamid teaches a method where the client executable matching program (i.e., biometric template) is downloaded by the client terminal from a remote memory (i.e., smart card) at the time of authentication [par. 23].

12. As to claim 12, Hamid teaches a method where the authentication result is used to authenticate a user for authorizing a secure transaction [par. 25].

13. As to claim 13, Hamid teaches a method where the secure transaction is controlled by an executable transaction program stored on the user-presented device [par. 64].

14. As to claim 14, Hamid teaches a method where when the authentication result indicates an adequate match, a first security access check key (e.g., image portion) is constructed including the authentication result [26, fig. 3]

15. As to claim 15, Hamid teaches a method where a second security access check key is requested and compared with the first security access key (e.g., image portion),the result of said comparison being used to enable the executable transaction program if it yields a positive authentication result [28, 29, fig. 3].

16. As to claim 16, Hamid teaches a method where the second security access check key (e.g., image portion) is issued from a security server [28, fig. 3].

17. As to claim 17, Hamid teaches a method where the first and second security access check keys each include a unique identification number [24, fig. 3].

18. As to claim 18, Hamid teaches a method where the unique identification number contains a number obtained from a mathematical operation on a randomly generated number and the authentication result [par. 48].

19. As to claim 19, Hamid teaches a method where the randomly generated number changes at each time the number is used [par. 55].

20. As to claim 20, Hamid teaches a method where the changing random number is tracked by dividing the number into two portions, a first portion to be used as the current random number and a second portion to be used as the next random number [par. 47].

21. As to claim 21, Hamid teaches a method where the unique identification number contains a number that is remembered by the user [par. 27].

22. As to claim 22, Hamid teaches a method where more than one authentication methods can be used to obtain the authentication result, each being incorporated into the unique identification number (par. 27).

23. As to claim 23, Hamid teaches a method where the access is divided into several levels and wherein the level of access granted to a user is dependent on the confidence level of positive identity obtained from the unique identification number (i.e., ... teaches a multiple security level using PIN and biometric authentication [par. 27]).

24. As to claim 24, Hamid teaches a system for authenticating a user according to a biometrics parameter of the user, the system comprising: a user-presented device (i.e.,

smart card) on which is stored a biometrics identification template divided into a secure portion and an open portion [par. 26], where only said open portion can be transmitted out of the said device; an authentication device (i.e., smart card reader interface) operable to read biometrics data derived from a user [25, fig. 3], where only said open portion is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template (i.e., ... teaches providing a public portion from a smart card for which is preprocessed registered biometric data [par. 26-27]), an authentication device operable to read biometric data derived from a user [par. 27], and comprising means for communicating with the user-presented device and a client terminal (par. 23) a client terminal arranged to receive the said open portion of the biometrics identification template held on the user-presented device (i.e., smart card) and the biometrics data derived from the user, and comprising a client processor operable to implement a first stage of biometric identity authentication process between said derived data and said open portion to produce intermediate results [par. 27], and to transmit the intermediate results of said biometric identity authentication process to the user-presented device [28, fig. 3], wherein said intermediate results (e.g., image portion) comprise parameters for alignment of said derived data and said biometric identification template (i.e., ... teaches a providing a image portion extracted from an aligned image from which a derived private portion was constructed [par. 27]); and wherein the user-presented device (i.e., smart card) comprises a device processor operable to implement a second stage of the

biometric identity authentication process to complete the biometric identity authentication process using said intermediate results and secure portion and to issue a biometric authentication result based thereon (to provide a smart card biometric authentication capability [col. 7, lines 60-67]).

25. As to claim 25, Hamid teaches a system where the secure portion of the biometrics identification template is the portion containing data unauthorized modification of which may cause the system to incorrectly authenticate an impostor as a genuine user [par. 23].

26. As to claim 26, Cancelled

27. As to claim 27, Hamid teaches a system where the biometrics parameter is a fingerprint, and where the authentication device includes a fingerprint Sensor (par. 23).

28. As to claim 28, Cancelled.

29. As to claim 29, Hamid teaches a system where the user-presented device (i.e., smart card) comprises a memory (i.e., micro chip) in which is stored a local executable matching program (i.e., application) for implementing the second stage of the matching process [par. 64].

30. As to claim 30, Hamid teaches a system where the memory on the user-presented device stores a client executable matching program which is transmitted to the client processor to implement the first stage of the matching process (par. 23).

31. As to claim 31, Hamid teaches a system which comprises a security server connected to the client terminal [par. 64].

32. As to claim 32, Hamid, teaches a system where the security server (i.e., host processor) holds a client executable matching program for implementing the first stage of the matching process [par. 23].

33. As to claim 33, Hamid teaches a system where the security server holds a security access check key requestable (e.g., biometric sample) by the client terminal for enabling a transaction [par. 64].

34. As to claim 34, Hamid teaches a system which comprises a transaction server arranged to implement secure transactions and which is in communication with the client terminal so that the authentication result is usable to authenticate a user for authorizing a secure transaction [par. 25].

35. As to claim 35, Hamid teaches a system where the user-presented device stores an executable transaction program (i.e., biometric data) for controlling the secure transaction (par. 64).

36. As to claim 36, Hamid teaches a system where more than one authentication methods can be used to obtain the authentication result (par. 27).

37. As to claim 37, Hamid teaches a system where the access to the transaction server is divided into several levels and wherein the level of access granted to a user is dependent on the confidence level of positive identity obtained based on the results from the various authentication methods used (par. 27).

38. Claims 38-43, 45-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Studd in view of Hamid and further in view of Larsson.

39. As to claim 38, Studd teaches a method of executing an operation using first and second processors, the method comprising: storing in the first processor a first task table containing a plurality of process names (i.e., mobile device application) with associated process identifiers, each associated with a process locator (i.e., Studd teaches a request for a list of mobile device application from mobile to device for which said mobile device application will be stored and executed [par. 51]);

storing in the second processor a second task table containing said of process names and process identifiers (i.e., Studd teaches a mobile device containing list mobile device application [par. 51]); identifying at the second processor a process to be executed and issuing a request to the first processor to execute said process (i.e., Studd teaches identifying a mobile application to execute [par. 51 - par. 53]); locating said process using the process locator and executing said process at the first processor to generate a result [par. 51 - par. 53]; and returning the result to the second processor [par. 51 - par. 53]. Studd does not expressly teach: wherein the operation being executed is a fingerprint- matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor, wherein the base minutiae finding process is a first stage of a biometric identity authentication process implemented between data derived from a user biometric parameter and an open portion of a biometric identification template wherein the biometric identification template is divided into the open portion and a secure portion to produce intermediate results, wherein the biometric identification template is divided into the open portion and a secure portion and said intermediate results comprise parameters for alignment of said data and said biometric identification template and are transmitted from the first processor to the second processor, and wherein the minutiae matching process is a second stage of the biometric identity authentication process to issue a biometric authentication result using the intermediate results. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Studd as introduced by Hamid. Hamid discloses: wherein the

operation being executed is a fingerprint- matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor (to provide a fingerprint minutiae matching algorithm [col. 7, lines 20- 51]), wherein the base minutiae finding process is a first stage of a biometric identity authentication process implemented between data derived from a user biometric parameter and an open portion of a biometric identification template wherein the biometric identification template is divided into the open portion and a secure portion to produce intermediate results (to provide a transmitting capability from a smart card a public portion (e.g., open) to a host computer for the purpose of authentication [par. 27], and said intermediate results comprise parameters for alignment of said data and said biometric identification template and are transmitted from the first processor to the second processor, and wherein the minutiae matching process is a second stage of the biometric identity authentication process to issue a biometric authentication result using the intermediate results (to provide processing at the host for biometric authentication [26, 27, fig. 3]]. Therefore, given the teachings of Hamid, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Studd by employing the well known features of a fingerprint matching algorithm disclosed above by Hamid, for which distributed authentication will be enhanced [col. 7, lines 20-51].

Although the combination of Studd and Hamid discloses a public portion (e.g. open portion), the combination of Studd and Hamid does not expressly recite open portion

containing a subset of minutiae data selected such that the content of the open portion is insufficient to construct a fake template that would allow an impostor to be incorrectly authenticated as a genuine user. The Examiner respectfully submits at the time of applicant's original filings Larsson disclosed a template residing on a smart card and the use of a subset of the biometric data as part of the biometric authentication process [par. 38]. Therefore given Studd and Hamid use of a smart card containing biometric data a person having ordinary skill in the art would have recognize the advantage of modifying the combination of Studd and Hamid to enhance the security biometric authentication process with the feature of using a subset of the biometric data for authentication purposes as disclosed by Larsson.

40. As to claim 39, Studd teaches a method where said process names (i.e., identifiers) include object names associated with respective object identifiers [par. 51, lines 7-10].

41. As to claim 40, Studd teaches a method where each object has associated therewith a plurality of functions (i.e., mobile device application) each identified by function names and associated function identifiers in the first and second task tables (par. 51).

42. As to claim 41, Studd teaches a method where the process locator identifies (i.e., identifier) the starting address of a process in a program memory (par. 51, lines 7-10).

43. As to claim 42, Studd teaches a method where the second processor has significantly less processing power than the first processor (par. 29, lines 8-11).

44. As to claim 43, Studd teaches a method where the second processor is arranged to execute locally processes requiring less processing power than those executed by the first processor [fig. 5].

45. As to claim 45, Studd teaches a method where there are a plurality of second processors in communication with a single first processor, each second processor holding a respective task table, and the first processor holding a first task table (i.e., mobile device application) including all processes identified by the task tables of the second processors (i.e., Studd teaches a mobile device with a list of mobile device applications [par. 50- par. 53]).

46. As to claim 46, Studd teaches a method where a client bridge (i.e., predetermine mechanism) is connected between the first and second processors, the client bridge (i.e., predetermine mechanism) conveying said requests from the second processor to the first processor and returning the results from the first processor to the second processor (par. 100).

47. As to claim 47, Studd teaches a method where the first processor is a client terminal and the second processor is embedded on a secure portable computing and data storage platform [404, fig. 4].

48. As to claim 48, Studd teaches a method where there are a plurality of first processors connected (i.e., multiple processors) via a client bridge to one or more second processor and arranged to implement different subsets of the processes in the task table of the second processor [par. 29, lines 7-11].

49. As to claim 49, Studd teaches a processing system comprising: a first processor in which is stored a first task table containing a plurality of process names and process identifiers, each associated with a process locator (i.e., Studd teaches a request for a list of mobile device application from mobile to device for which said mobile device application will be stored and executed [par. 51]); a second processor in which is stored a second task table containing said process names with associated process identifiers (i.e., Studd teaches a mobile device containing list mobile device application [par. 51]);
50. the second processor including a distributed object execution manager for identifying a process to be executed and issuing a request to the first processor to execute said process (i.e., Studd teaches identifying a mobile application to execute [par. 51 - par. 53]); and the first processor including a client distributed object execution manager for controlling the execution of said processes at the first processor, the results of execution of the processes implemented at the first processor being returned

to the second processor [par. 51 - par. 53]. Studd does not expressly teach: wherein the operation being executed is a fingerprint- matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor, wherein the base minutiae finding process is a first stage of a biometric identity authentication process implemented between data derived from a user biometric parameter and an open portion of a biometric identification template wherein the biometric identification template is divided into the open portion and a secure portion to produce intermediate results, and said intermediate results comprise parameters for alignment of said data and said biometric identification template and are transmitted from the first processor to the second processor, and wherein the minutiae matching process is a second stage of the biometric identity authentication process to issue a biometric authentication result using the intermediate results. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Studd as introduced by Hamid. Hamid discloses: wherein the operation being executed is a fingerprint-matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor (to provide a fingerprint minutiae matching algorithm [col. 7, lines 20- 51]), wherein the base minutiae finding process is a first stage of a biometric identity authentication process implemented between data derived from a user biometric parameter and an open portion of a biometric identification template wherein the biometric identification template is divided into the open portion and a secure portion to produce intermediate

results (to provide a transmitting capability from a smart card a public portion (e.g., open) to a host computer for the purpose of authentication [par. 27]), and said intermediate results comprise parameters for alignment of said data and said biometric identification template and are transmitted from the first processor to the second processor, and wherein the minutiae matching process is a second stage of the biometric identity authentication process to issue a biometric authentication result using the intermediate results (to provide processing at the host for biometric authentication [26, 27, fig. 3]]. Therefore, given the teachings of Hamid, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Studd by employing the well known features of a fingerprint matching algorithm disclosed above by Hamid, for which distributed authentication will be enhanced [col. 7, lines 20-51]. Although the combination of Studd and Hamid discloses a public portion (e.g. open portion) [Hamid par. 26], the combination of Studd and Hamid does not expressly recite open portion containing a subset of minutiae data selected such that the content of the open portion is insufficient to construct a fake template that would allow an impostor to be incorrectly authenticated as a genuine user. The Examiner respectfully submits at the time of applicant's original filings Larsson disclosed a template residing on a smart card and the use of a subset of the biometric data as part of the biometric authentication process [par. 38]. Therefore given Studd and Hamid use of a smart card containing biometric data a person having ordinary skill in the art would have recognize the advantage of modifying the combination of Studd and Hamid to enhance the security biometric authentication process with the feature of

using a subset of the biometric data for authentication purposes as disclosed by Larsson.

51. As to claim 50, Studd teaches a processing system where the first processor includes a client manager (i.e., input/output controller hub) for handling communications between the first and second processors (par. 31).

52. As to claim 51, Studd teaches a system where the first processor includes an execution manager (i.e., framework application services unit) for handling the execution of processes (i.e., mobile device application) [par. 51 - par. 53]. 54. As to claim 52, Studd teaches a system where the first processor comprises a program store for holding said processes, the process locator (i.e., identifier) being used to identify the location of said processes in the program store [par. 51].

53. As to claim 53, Studd teaches a system where the second processor includes a remote device manager for transmitting said requests to the first processor [fig. 4].

54. As to claim 54, Studd teaches a system where the second processor comprises a stack for holding results returned to it from the first processor (par. 61).

55. As to claim 55, Studd teaches a system according where the second processor includes a program store for holding said processes (par. 51).

56. As to claim 56, Studd teaches a system where the first processor comprises a client terminal (fig. 4).

57. As to claim 57, Studd teaches a system which comprises a plurality of first processors, the system further comprising a client bridge (i.e., predetermine mechanism) for handling communications between the first processors and the second processor [par. 100].

58. As to claim 58, Studd teaches a system where each first processor comprises a server (par. 100, lines 6-9).

59. As to claim 59, Studd teaches a system where the client bridge includes a network execution manager (i.e., input/output controller hub) for transmitting requests from the second processor to the appropriate one of the first processors, based on a processor identifier in the request [par. 31, lines 1-8].

60. As to claim 60, Studd teaches a system comprising a plurality of second processors and a client bridge (i.e., predetermine mechanism) for connecting said second processors to said first processor [par. 100, lines 1-9].

61. As to claim 61, Studd teaches a system where the second or each second processor is embedded on a respective portable secure computing and data storage platform such as smart card [par. 404, fig. 4].

Response to Amendment

Examiner Remarks – Applicant's arguments submitted on 9/8/2010

Applicant argues:

> "... Neither Hamid or Larsson teach or suggest that an open portion of a user's biometric identification template is insufficient to construct a fake template that would allow an imposter to be incorrectly authenticated."

The Examiner respectfully submits Larson specifically teaches a template divided into a public part and a private part. See Larson paragraph 50. The Examiner notes that applicant claims a template divided into an open and secure part. See applicant's claim 49. Larson further states that the biometric authentication data comprises a public and private part corresponding to the template's public and private part biometric authentication data. See Larson paragraph 50.

The Examiner respectfully submits that the public part is subset data corresponding to biometric authentication data needed to fully authenticate a subject and the private part is subset data corresponding to biometric authentication data needed to fully authenticate a subject and that as a whole this template data is used to fully

authenticate a subject. See Larson paragraph 49-64. The Examiner contends that based on Larson's teachings, just using either the public part of the template or the private part of the template is not sufficient to fully authenticate a subject and that a would be impostor (e.g., person attempting to fraudulently by-pass Larson's system) would need both parts to be successful at a by-pass attempt.

Examiner Remarks – Affidavit

The affidavit filed on 11/22/2010 under 37 CFR 1.131 has been considered but is ineffective to overcome the Hamid, Larson and Studd prior art references.

Applicant argues:

> "**Applicants submit herewith a declaration under 37 C.F.R. 1.131 along with the original annotated source code (Exhibit i), commented source code (Exhibit 2) and a screen shot (Exhibit 3) of the directory holding the source code. The declarant asserts and the exhibits support the assertion that the annotated source code (Exhibit i) was prepared as discussed in the declaration and was operational in April 2001 showing actual reduction to practice of the claimed invention before the filing dates of any of the cited references. The commented source code (Exhibit 2) contains comments in bold prepared for the examiner's convenience to follow the claim limitations. The commented version of the source code clearly shows all the elements of the pending claims and thus fully supports the declaration of the inventor. Larsson was filed July 5, 2001 and as the annotated source code (Exhibit i) proves, the limitations of the present claims were incorporated in the source code in April 2001, several months before the filing of Larsson. Thus, Larsson is not available as prior art. The actual reduction to practice also predates the filing date of Hamid and its parent application issued to Hillhouse, et al., Method and Apparatus for Supporting a Biometric Registration Performed on a Card, U.S. Patent 7,274,807 (Sep. 25, 2007) (Hereinafter Hillhouse). The priority date of Hillhouse is May 30, 2002. Accordingly, even Hillhouse (of which the cited Hamid reference is a CIP) is not prior art. Thus, neither Hamid nor its parent, Hillhouse, are available for use as prior art in rejecting the claims of**

the present application. Accordingly, Applicants respectfully request that the rejections of claims i, 2, 3, 5, 7 through 25, 27 and 29 through 37 be withdrawn. Claims 38 through 43 and 45 through 61 stand rejected under 35 USC § 103(a) as unpatentable over Studd, Method and System for Executing Applications on a Mobile Device, U.S. Patent Application Publication 2004/0122774 (Jun. 24, 2004) in view of Hamid and further in view of Larsson. As discussed above, Larsson is not available as prior art and thus this rejection should be withdrawn. The earliest priority date for Studd is August 2, 2002 over a year after the date of applicant's actual reduction to practice. Thus, Studd is also not available as prior art and this rejection should be withdrawn."

The Examiner respectfully submits that per MPEP 715.04, 131 affidavits have to be from ALL inventors unless there is something that shows that the rejected claims are only from the 1 inventor that signed the affidavit. The Examiner respectfully draws applicant's attention to Exhibit 2, page 1. In the program notation section, Lawrence Chen is solely named as author. The Examiner notes that on the Oath and Declaration, there are two signed inventors, Tai Pang Chen and Wei Yum Yau.

Additionally on page 28 of Exhibit 1, a JIANG XUDONG is stated to be the author of at least what appears to be program logic for matching the minutiae. The Examiner notes that JIANG XUDONG does not appear as a signed inventor on the Oath and Declaration. Additionally, in Exhibit 2, page 26 and 27 JIANG XUDONG name appear as the author of program code relating to aligning and matching minutiae. The Examiner contends that if JIANG XUDONG is an inventor, than applicant's rep must make the record clear of this matter.

The Examiner respectfully submits the source code contained in Exhibit 1 as proof that applicant had possession of the claim subject matter has no comments/remarks/notations that explains how the source code supports the claim subject matter. As such the content of Exhibit 1 cannot be properly construed by the Examiner to properly support the claim limitations as presented on 9/8/2010.

With regards to the source code contained in Exhibit 2, the Examiner contends that the applicant claims an open and private portion of a biometric template. The Examiner respectfully contends that simply notating the method signature with remarks is not sufficient. Refer to pages 1 thru 3 of Exhibits 2. Examiner cannot construe a method signature notation as support for the claimed subject matter. Additionally review of the actual method body of "save_base_template" on pages 16 and 17 the method body simply illustrates handling an exception. The Examiner notes that it is unclear how the source code referenced (e.g., highlighted block of code [page 17]) supports applicant's claim limitation element "open portion". On page 19 of Exhibit 2 the applicant notates another method signature, "main_template" to correspond to subject matter relating too the secure portion of the biometric template. Again the Examiner cannot properly determine how the method signature of "main_template" supports the claimed limitation element of secure portion.

As noted above the Examiner contends the evidence submitted both Exhibits 1 & 2 are insufficient to establish a reduction to practice of the invention in this country or a

NAFTA or WTO member country prior to the effective date of the prior art of Hamid, Larson and Studd. Moreover the affidavits do not comply with MPEP 715.04 and the inventorship appears to be incorrect. Therefore the Examiner maintains the 103(a) rejection made under prior art references Hamid, Larsson and Studd.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431